

# การพิสูจน์ตัวตนโดยจังหวะการพิมพ์ด้วยวิธีการวัดความต่างของเส้นโคจร

## Keystroke Dynamics Authentication with Trajectory Dissimilarity

เกษม หวังสุข และ ธนภัทร์ อนุศาสน์อมรกุล  
ภาควิชาวิทยาการคอมพิวเตอร์และสารสนเทศ  
คณะวิทยาศาสตร์ประยุกต์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ  
Email: digital\_hyper@hotmail.com1,tanapata@kmutnb.ac.th2

### บทคัดย่อ

การพิสูจน์ตัวตนบนระบบคอมพิวเตอร์ในปัจจุบันใช้ระบบ Username และ Password ซึ่งระบบดังกล่าวยังมีจุดอ่อนเนื่องจาก Username ถูกเปิดเผยได้โดยง่าย และผู้โจมตีเพียงคาดเดา Password เท่านั้น งานวิจัยนี้จึงมีแนวคิดที่จะเสริมความแข็งแกร่งของระบบโดยการผนวกจังหวะการพิมพ์ (Keystroke Dynamics) ซึ่งเป็นมาตรวัดทางชีวแบบพฤติกรรมอย่างหนึ่งเข้าไปกับ Username เนื่องจาก Password มีการเปลี่ยนแปลงอยู่บ่อยครั้งตามนโยบายความปลอดภัยในขณะที่ Username จะไม่มีการเปลี่ยนแปลง โดยได้นำเสนอการวิเคราะห์และศึกษาพฤติกรรมจังหวะการพิมพ์ของ Username ที่มีขนาดข้อมูลตัวอย่างค่อนข้างเล็กและประยุกต์ใช้การวิเคราะห์ความแตกต่างของเส้นโคจร เพื่อใช้เป็นอัลกอริทึมหลักในการพิสูจน์ตัวตน รวมทั้งได้แสดงวิธีการเลือก Feature ของจังหวะการพิมพ์ เพื่อนำมาประกอบเป็นเส้นโคจรที่ให้ผลการพิสูจน์ตัวตนที่มีประสิทธิภาพสูง โดยมีความถูกต้อง 96% หรือมีความผิดพลาด 4%

### คำสำคัญ

การพิสูจน์ตัวตน จังหวะการพิมพ์

### Abstract

From a typical authentication scheme, a username and a password are used for user verification process. However, the scheme still has some weaknesses because a username is not secret and an imposter can guess a password to break into the system. Our research focuses on this weakness and tries to improve security level of this system by combining keystroke dynamics into the system. A username is normally unchanged but a password should be changed regularly for security purposes. Therefore, we propose to investigate a keystroke dynamics profile of a username with a small set of sample data and use trajectory dissimilarity for the main algorithm for authentication verification. We also propose a method for keystroke dynamics feature selection to build a trajectory profile which gives authentication accuracy 96% or 4% equal error rate (ERR).

## Keywords

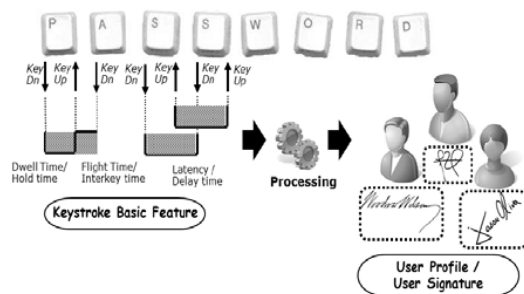
authentication, keystroke dynamics

### 1. คำนำ

ในปัจจุบันระบบคอมพิวเตอร์ได้เข้ามามีบทบาทสำคัญ ส่งผลให้การรักษาความปลอดภัยบนระบบคอมพิวเตอร์เพื่อรักษาสิทธิและข้อมูลของผู้ใช้งานมีความสำคัญมากขึ้นเช่นกัน การพิสูจน์ตัวตนบนระบบคอมพิวเตอร์ด้วย Username และ Password เป็นวิธีการที่ใช้อย่างแพร่หลายในระบบคอมพิวเตอร์เกือบทุกระบบ ซึ่งระบบการพิสูจน์ตัวตนดังกล่าวยังมีจุดอ่อน เนื่องจากผู้โจมตีสามารถคาดเดา Password ให้ถูกต้องเท่านั้น และ Username ไม่เป็นความลับคาดเดาได้ง่าย งานวิจัยนี้จึงได้มีแนวคิดโดยใช้ Username ผสมกับรหัสลับบางอย่างที่เป็นความลับต่อผู้โจมตีได้ง่าย และไม่ต้องจดจำสำหรับผู้ใช้เป็นเจ้าของตัวจริง จึงนำมาซึ่งการใช้จังหวะการพิมพ์ (Keystroke Dynamics) ซึ่งเป็นมาตรวัดทางชีวแบบพฤติกรรม ซึ่งต้องการ Hardware เพียงแป้นพิมพ์ (Keyboard) เท่านั้น [1]

Keystroke Dynamics เป็นหลักการที่ตั้งอยู่บนพื้นฐานของเวลาในการกดคีย์บนแป้นพิมพ์ (Keyboard) ซึ่งตั้งสมมติฐานว่าจังหวะการพิมพ์ของแต่ละคนจะมีลักษณะเฉพาะตัวและสามารถนำมาใช้ในระบบการพิสูจน์ตัวตนได้ Feature พื้นฐานของ Keystroke Dynamics [1] มีดังนี้ Key Hold Time: เวลาที่กดคีย์ค้างไว้ โดยจับเวลาตั้งแต่เริ่มกดคีย์จนกระทั่งปล่อยคีย์ Interkey Time: เวลาที่เปลี่ยนคีย์ใดไปสู่อีกคีย์หนึ่งซึ่งอาจได้เป็นตัวเลขค่าบวกหรือลบ กรณีที่ได้ค่าบวกคือมีการปล่อยคีย์ก่อนหน้าก่อนที่จะ

กดคีย์ถัดไป หากได้ค่าลบคือมีการกดคีย์ถัดไปก่อนที่จะปล่อยคีย์ก่อนหน้า หรือมีการกดคีย์ซ้อนกันในช่วงเวลาที่เปลี่ยนคีย์ Latency: เวลาที่เริ่มกดคีย์จนกระทั่งกดคีย์ถัดไปหรืออีกนัยหนึ่งคือเวลาที่เริ่มจากปล่อยคีย์จนกระทั่งปล่อยคีย์ถัดไปซึ่งสามารถอธิบายให้เข้าใจได้ง่ายขึ้นดังภาพที่ 1 จากแนวคิดและ Feature พื้นฐานดังกล่าวงานวิจัยนี้ได้สร้าง Feature เพิ่มเติมจาก Feature พื้นฐาน เพื่อนำมาวิเคราะห์และหา Feature ที่ดีที่สุด จากนั้นจะนำมาประกอบกันเป็นเส้นโคจรและประมวลผลการระบุตัวตนด้วยวิธีการวัดความต่างของเส้นโคจร (Trajectory) ซึ่งจะได้กล่าวถึงรายละเอียดในลำดับถัดไป



ภาพที่ 1 หลักการพื้นฐานและ Feature ของ Keystroke Dynamics

หัวข้อถัดไปจะกล่าวถึงงานวิจัยที่เกี่ยวข้อง หลังจากนั้นจะอธิบายวิธีการรวบรวมข้อมูล Keystroke Dynamics และการสร้าง profile ของเส้นโคจร ถัดมาจะนำเสนอวิธีการระบุตัวตนด้วยเส้นโคจร วิธีการเลือก feature และการวิเคราะห์และเปรียบเทียบผลการทดลอง และสรุปผลการทดลองในหัวข้อสุดท้าย

## 2. งานวิจัยที่เกี่ยวข้อง

Keystroke Dynamics Authentication (KDA) ยังมีข้อบกพร่องในด้านของความแปรปรวนและความไม่เสถียรของจังหวะการพิมพ์ของผู้ใช้งานจึงทำให้มีผู้วิจัยหลายท่านคิดค้นและนำเทคนิคหลากหลายเข้ามาประยุกต์กับ KDA เพื่อทำให้เสถียรยิ่งขึ้นอย่างเช่น Haider และ Abbas [2] ได้นำเสนอ Neural Network, Fuzzy Classification, Basic Statistic รวมถึงการใช้เทคนิคขั้นสูงทางด้าน Artificial Intelligence อย่างเช่น Senathipathi และ Batri [3] นำเสนอ Genetic Algorithm และ SVM เข้ามาผสมผสานกัน รวมถึงยังมีแนวคิดเพื่อขจัดความแปรปรวนข้อมูลเช่น Kaneko, Kinpara และ Shinomi [4] นำเสนอ Hamming Distance มาเป็นตัวคัดกรองข้อมูลที่มีความแปรปรวนออกจากระบบ เพื่อให้การประมวลผลและการระบุตัวตนแม่นยำยิ่งขึ้น อย่างไรก็ตามเทคนิคแต่ละแบบที่นำมาใช้กับ KDA นั้นมีทั้งข้อดีและข้อเสียอย่างเช่น Basic Statistic[2] มีข้อดีคือมีความเรียบง่าย ใช้เวลาในการคำนวณน้อย รวมถึงใช้พื้นที่ในการเก็บข้อมูลที่ใช้เป็น Profile ของผู้ใช้เพียงเล็กน้อย แต่พบข้อเสียตรงที่ความแปรปรวนของข้อมูลอาจทำให้การพิสูจน์ตัวตนไม่มีประสิทธิภาพตามที่ต้องการ

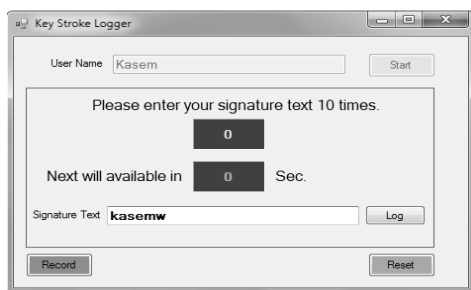
หากกล่าวถึงด้านประสิทธิภาพในการพิสูจน์ตัวตนของแต่ละงานวิจัยพบว่ามีความหลากหลายต่างกันไปเช่น Limpanuparb [1] ซึ่งใช้อาสาสมัครจำนวน 17 คน และใช้การผสมผสานเทคนิคทางสถิติ CAV, PMAS และปรับปรุงประสิทธิภาพโดยเพิ่มตัวแปรในการคำนวณจาก 1 ตัวแปรเป็น 2 ตัวแปรซึ่งทำให้มีประสิทธิภาพสูงคือมีความแม่นยำถึง 94.76% หรือมีความผิดพลาด 5.24% โดยที่ตัวแปรที่ใช้ในการคำนวณทั้งสองนั้นต้องค้นหาค่าที่เหมาะสมแบบ

Exhaustive ซึ่งอาจทำให้ใช้เวลามากในการค้นหา แต่มีข้อดีตรงที่วิธีการไม่ซับซ้อนจนเกินไปและอาจนำไปใช้ได้จริง Kang, Hwang, และ Cho [5] ซึ่งใช้ข้อมูลจากอาสาสมัครจำนวน 21 คน และใช้เทคนิค Classification ด้วย K-Mean ผสมผสานกับการเรียนรู้เมื่อเวลาผ่านไปด้วยวิธีการ Moving Window และ Growing Window ทำให้มีข้อดีตรงจุดที่สามารถรักษาประสิทธิภาพของระบบได้เมื่อเวลาผ่านไป จากวิธีการดังกล่าวได้ให้ผลประสิทธิภาพของระบบที่มีความถูกต้องถึง 96.2% หรือมีความผิดพลาดที่ 3.8% แต่ด้วยหลักการเรียนรู้แบบ Windows ผสมผสานกับการ Classification นั้นนำมาซึ่งความต้องการพื้นที่ในการเก็บ Pattern ของผู้ใช้งานแต่ละคนซึ่งเป็นจุดด้อยที่ต้องคำนึงถึง หากนำไปใช้งานกับระบบจริงที่มีผู้ใช้งานจำนวนมาก ผู้วิจัยจึงได้ศึกษาเทคนิคดังกล่าวเพื่อนำมาประยุกต์ใช้กับโครงการวิจัยได้อย่างเหมาะสม

## 3. รวบรวมข้อมูล Keystroke Dynamics

ผู้วิจัยได้ออกแบบและพัฒนาโปรแกรมประยุกต์สำหรับเก็บข้อมูล Keystroke Profile ของ Username จากอาสาสมัครจำนวน 20 คนดังแสดงในภาพที่ 2 ซึ่งจะกำหนดให้แต่ละคนพิมพ์ Username จำนวน 3 ชุด แต่ละชุดจะกำหนดให้มีเวลาห่างกันอย่างน้อย 1 วัน เพื่อวิเคราะห์ถึงความแปรปรวนเมื่อเวลาผ่านไป เพื่อให้สอดคล้องกับการใช้งานในระบบจริง ในการพิมพ์แต่ละชุดข้อมูลจะกำหนดให้อาสาสมัครพิมพ์ Username จำนวน 10 ครั้ง ซึ่งแต่ละครั้งจะถูกห้วงเวลาให้ห่างกันอย่างน้อย 5 วินาที เพื่อลดความแปรปรวนของพฤติกรรมในขณะที่พิมพ์โดยรูปแบบของ Username ที่กำหนดให้พิมพ์นั้นจะใช้รูปแบบ Username กำหนดเป็นชื่อภาษาอังกฤษแล้วตามด้วย

อักขรภาษาอังกฤษตัวแรกของนามสกุล เช่นชื่อ Kasem Wangsuk จะถูกกำหนดเป็น Username “kasemw” โดยมีสมมติฐานว่าสิ่งที่ผู้ใช้งานที่คุ้นเคย ย่อมนำมาซึ่งความคงที่ ความเป็นเอกลักษณ์และความ เป็นตัวตนที่ดี ซึ่งมีขั้นตอนการเก็บข้อมูลดังนี้



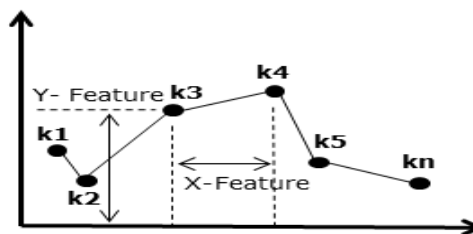
ภาพที่ 2 โปรแกรมประยุกต์ที่ใช้ในการเก็บข้อมูล

อาสาสมัครแต่ละคนพิมพ์ข้อมูลคนละ 3 ชุด แต่ละชุด ประกอบด้วยข้อมูล Username จำนวน 10 ครั้ง ซึ่งทำให้แต่ละคนมีข้อมูล Username จำนวน 30 ครั้ง นำข้อมูลชุดแรกมาสร้างเป็น Profile ต้นแบบของอาสาสมัครแต่ละคน ส่วนข้อมูลที่เหลืออีก 2 ชุด จะนำมาวัดประสิทธิภาพ (รายละเอียดจะกล่าวในหัวข้อถัดไป) ผู้วิจัยได้แต่งตั้งผู้กระทำการเป็นผู้โจมตี (Imposter) จำนวน 3 คน แต่ละคนจะพิมพ์ Username ของอาสาสมัครทุกคนจำนวนคนละ 1 ชุด ซึ่งทำให้อาสาสมัครแต่ละคนมีข้อมูลการถูกปลอมแปลงจำนวน 3 ชุด หรือ 30 ครั้ง เมื่อเก็บข้อมูลจนครบจะมีข้อมูลของอาสาสมัครแต่ละคนจำนวน 6 ชุด หรือ 60 ครั้ง ซึ่งแบ่งเป็นข้อมูลของเจ้าของ 3 ชุด หรือ 30 ครั้ง และข้อมูลของการถูกผู้โจมตีอีก 3 ชุด หรือ 30 ครั้ง เมื่อเก็บข้อมูลอาสาสมัครครบทั้ง 20 คน ทำให้มีข้อมูลมากถึง 1,200 ครั้ง

#### 4. การสร้าง Profile ของเส้นโคจร

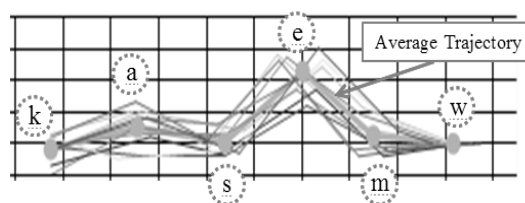
Profile ต้นแบบถูกสร้างจากข้อมูลชุดแรกเพื่อ

ทำให้ระบบสมจริงจากแนวคิดที่ว่า Profile ควรจะเก็บครั้งแรกที่เข้าใช้ ข้อมูลชุดแรกคือ Username ทั้ง 10 ครั้ง จะถูกนำมาแปลงเป็นเส้นโคจร โดยมีการเลือก Feature ของข้อมูล Keystroke Dynamics ที่ได้มาเป็นพิกัด (Coordinate) ของเส้นโคจรในแต่ละจุดตามแนวคิดดังภาพที่ 3 โดยการพิมพ์ Username แต่ละครั้งจะได้เส้นโคจร 1 เส้น และแต่ละจุดบนเส้นคือแต่ละตัวอักษรบน Username นั้น พิกัดของแต่ละจุดจะถูกเลือกและสกัดมาจาก Feature ของข้อมูล Keystroke ของแต่ละ Key โดยจะกำหนดพิกัดในระดับ 2 มิติคือทั้งแกน X และแกน Y เพื่อความหลากหลายและแตกต่างจากงานวิจัยอื่น [4] ให้เสมือนเป็นเส้นโคจรที่ใกล้เคียงความเป็นจริงที่มีระยะ X และ Y ของแต่ละจุดผันผวนไปไม่เท่ากัน



ภาพที่ 3 แนวคิดการแปลงข้อมูลของ Keystroke เป็นเส้นโคจร

เมื่อได้ข้อมูลเส้นโคจรทั้ง 10 เส้นจากข้อมูลชุดแรกจะนำมาสร้าง Profile เส้นโคจรต้นแบบเพียงเส้นเดียวเท่านั้น โดยนำเส้นโคจรทั้ง 10 เส้นมาหาค่าเฉลี่ยดังภาพที่ 4 ดังนั้นแต่ละอาสาสมัครจะมี Profile เส้นโคจรต้นแบบคนละ 1 เส้นเพื่อใช้ในการพิสูจน์ตัวตน



ภาพที่ 4 สร้างเส้นโคจรต้นแบบจากข้อมูลชุดแรก

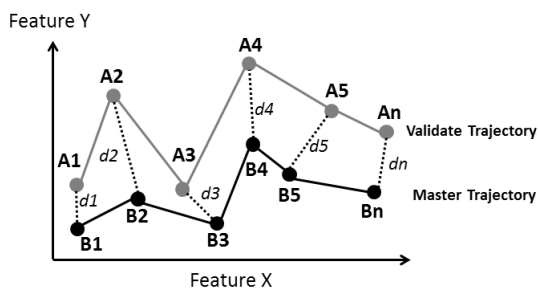
## 5. การระบุตัวตนด้วยการวัดความแตกต่างของเส้นโคจร

จากแนวความคิดในด้านการวัดความคล้ายของเส้นโคจร [6] ผู้วิจัยได้นำมาประยุกต์กับงานวิจัยชิ้นนี้ โดยสร้างเส้นโคจรต้นแบบ จากนั้นจะสร้างข้อกำหนดในการระบุตัวตนผู้วิจัยได้เลือกวิธีการวัดความแตกต่างด้วยผลรวมของระยะห่างของแต่ละจุดบนเส้นโคจรที่จะตรวจสอบกับเส้นโคจรต้นแบบที่เป็นเป้าหมายของการพิสูจน์ตัวตน จากนั้นจะพิจารณาว่าผลรวมของระยะห่างที่ได้เกินค่าที่กำหนดหรือไม่ ซึ่งจะกล่าวถึงรายละเอียดแต่ละส่วนดังนี้

### 5.1 การวัดความแตกต่างของเส้นโคจร

วัดผลรวมของระยะทางจุดต่อจุดของ Profile เส้นโคจรที่ต้องการตรวจสอบการพิสูจน์ตัวตนกับเส้นโคจรต้นแบบของเป้าหมายด้วยการวัดระยะทางแบบ Euclidean ซึ่งได้แนวคิดจากงานวิจัยที่นำเสนอโดย Laurinen, Siirtola และ Roning [6] ตามสมการที่ (1) และภาพที่ 5 เมื่อกำหนดให้จุด A1 ถึง An คือเส้นโคจรที่ต้องการตรวจสอบการพิสูจน์ตัวตน และกำหนดให้ B1 ถึง Bn คือเส้นโคจรต้นแบบ (Master Trajectory Profile) ซึ่งได้จากการเก็บข้อมูลในชุดแรกของผู้ใช้งาน Username

$$\text{Dissimilarity}_{(A,B)} = \sum_{i=1}^n \sqrt{(Ax_i - Bx_i)^2 + (Ay_i - By_i)^2} \quad (1)$$



ภาพที่ 5 วัดความแตกต่างของเส้นโคจรด้วย Euclidean

สมการจะวัดความแตกต่างของเส้นโคจรด้วยวิธีการคำนวณผลรวมของระยะห่างของแต่ละจุดบนเส้นโคจร โดยเทียบลำดับต่อจุด ซึ่งได้ตั้งสมมติฐานไว้ว่าหากเป็นเส้นโคจรที่มาจากเจ้าของเดียวกันจะต้องมีผลรวมของระยะทางที่ต่ำกว่าเส้นโคจรที่มาจากผู้ที่ต้องการโจมตี อย่างไรก็ตามวิธีการข้างต้นเป็นเพียงแค่การคำนวณการวัดความแตกต่างของเส้นโคจรเท่านั้น และยังไม่ใช่วิธีการตัดสินว่าเส้นโคจรที่เข้าตรวจสอบเป็นของใครเดียวกันหรือไม่แต่อย่างใด ซึ่งจะกล่าวถึงวิธีการและรายละเอียดตรงจุดนี้ในหัวข้อถัดไป

### 5.2 การระบุตัวตนด้วยความแตกต่างของเส้นโคจร

เมื่อกำหนดวิธีการวัดและคำนวณความแตกต่างของเส้นโคจรเสร็จสิ้น พบว่าวิธีการดังกล่าวเพียงแค่ให้ค่าระดับความแตกต่างออกมาเท่านั้น แต่ยังไม่สามารถระบุว่าเป็นเจ้าของที่แท้จริงหรือเป็นผู้โจมตีแต่อย่างใด ในส่วนนี้จะกล่าวถึงวิธีการระบุตัวตนการเป็นเจ้าของ Username ที่ชัดเจน จากหัวข้อที่ผ่านมาทำให้สามารถสร้าง Profile ของเส้นโคจรต้นแบบและการวัดความแตกต่างของเส้นโคจร โดยตั้งสมมติฐานว่ายิ่งค่าระดับความแตกต่างเข้าใกล้ศูนย์มากเท่าใดยิ่งแสดงความเป็นเจ้าของที่แท้จริงมากขึ้นเท่านั้น แต่ระดับความแตกต่างเท่าใดจึงจะเหมาะสมในการพิสูจน์ตัวตน ผู้วิจัยจึงนำเอาหลักการทางสถิติ [7] มาประยุกต์ใช้เป็นวิธีการพิสูจน์ตัวตนตามขั้นตอนดังนี้ คำนวณค่าระดับความแตกต่างของ Username ทั้ง 10 ครั้งของชุดแรก โดยเทียบกับเส้นโคจรต้นแบบที่ได้จาก Username ทั้ง 10 ครั้งของข้อมูลชุดเดียวกัน นำค่าระดับความแตกต่างที่ได้ของ Username ทั้ง 10 ครั้งมาหาค่าเฉลี่ย (Average) และค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) กำหนดสมการพิสูจน์ตัวตนดังสมการที่ (2) โดยกำหนดให้

$$f(x) = \begin{cases} 0; & \text{if } (A_{diss} > [B_{AvDiss} + (Sig * B_{StdDiss})]) \\ 1; & \text{if } (A_{diss} \leq [B_{AvDiss} + (Sig * B_{StdDiss})]) \end{cases} \quad (2)$$

Adiss คือ ค่าความต่างของเส้นโคจรที่จะตรวจสอบ การพิสูจน์ตัวตน BAvDiss คือ ค่าเฉลี่ยระดับความแตกต่างต่างของเส้นโคจรทั้ง 10 Username ที่ผู้เป็นเจ้าของได้เก็บเป็น Profile ไว้ BStdDiss คือ ค่าส่วนเบี่ยงเบนมาตรฐานความแตกต่างของเส้นโคจรทั้ง 10 Username ที่ผู้เป็นเจ้าของได้เก็บเป็น Profile ไว้ Sig คือค่า Allowance Factor ซึ่งเบื้องต้นจะกำหนดมีค่า 3.00 ตามทฤษฎี Six Sigma และปรับความเหมาะสมจากข้อมูลการทดลองของกลุ่มอาสาสมัครในลำดับถัดไป จากสมการที่ (2) เมื่อ  $f(x) = 0$  ระบบจะระบุว่าเป็นผู้โจมตี หรือไม่ใช่เจ้าของที่แท้จริงแต่หาก  $f(x) = 1$  ระบบจะระบุว่าเป็นเจ้าของที่แท้จริง

## 6. การคัดเลือก Feature เพื่อนำมาประกอบเป็นเส้นโคจร

จาก Feature พื้นฐานของ Keystroke Dynamics ผู้วิจัยได้นำเสนอ Feature เพิ่มเติมจาก Feature พื้นฐานมีรายละเอียดดังนี้ H/1000 คือการนำข้อมูลดิบ Hold Time ซึ่งมีหน่วยเป็น Millisecond ทำการ Normalize ให้เหลือค่าเป็นจุดทศนิยมโดยการหารด้วย 1000 เพราะข้อมูลส่วนใหญ่จะอยู่ในหลัก Milliseconds เท่านั้น การทำ Normalize เพื่อต้องการให้ Feature ทั้งหมดมีความสำคัญในระดับใกล้เคียงกัน I/1000 คือการนำข้อมูลดิบ Interkey Time ซึ่งมีหน่วยเป็น Millisecond มาทำการ Normalize ให้เหลือค่าเป็นจุดทศนิยม L/1000 คือการนำข้อมูลดิบ Latency Time ซึ่งมีหน่วยเป็น Millisecond มาทำการ Normalize ให้เหลือค่าเป็นจุดทศนิยม H/Total คือการนำข้อมูลดิบ Hold Time มีหน่วยเป็น Millisecond หารด้วยเวลาทั้งหมดที่พิมพ์ Username นั้น ผลลัพธ์ที่ได้จะเป็นเลขทศนิยมที่บ่งบอกถึงสัดส่วน

ของ Hold Time ของ key นั้นต่อเวลาทั้งหมดที่ทำการพิมพ์ Username นั้น I/Total คือการนำข้อมูลดิบ Interkey Time ซึ่งมีหน่วยเป็น Millisecond หารด้วยเวลาทั้งหมดที่พิมพ์ Username นั้น ผลลัพธ์ที่ได้จะเป็นเลขทศนิยม L/Total คือการนำข้อมูลดิบ Latency Time ซึ่งมีหน่วยเป็น Millisecond หารด้วยเวลาทั้งหมดที่พิมพ์ Username ชุดนั้น ผลลัพธ์ที่ได้จะเป็นเลขทศนิยม H/Sum H คือการนำข้อมูลดิบ Hold Time ซึ่งมีหน่วยเป็น Millisecond หารด้วยผลรวมของ Hold Time ทุกคีย์ ใน Username นั้น ผลลัพธ์ที่ได้จะเป็นเลขทศนิยมที่บ่งบอกถึงสัดส่วนของ Hold Time ของ key นั้นต่อ Hold Time ทั้งหมดที่พิมพ์ Username นั้น I/Sum I คือการนำข้อมูลดิบ Interkey Time ซึ่งมีหน่วยเป็น Millisecond หารด้วยผลรวมของ Interkey Time ทุกคีย์ใน Username นั้น ผลลัพธ์ที่ได้จะเป็นเลขทศนิยม L/Sum L คือการนำข้อมูลดิบ Latency Time ซึ่งมีหน่วยเป็น Millisecond หารด้วยผลรวมของ Latency Time ทุกคีย์ใน Username นั้น ผลลัพธ์ที่ได้จะเป็นเลขทศนิยม อย่างไรก็ตามในการสร้างเส้นโคจรต้องการเพียงแค่ Feature 2 ตัวเท่านั้น เพื่อนำมาสร้างฟังก์ชันเส้นโคจร X,Y ซึ่งผู้วิจัยได้คิดค้นวิธีการวัดประสิทธิภาพของ Feature แต่ละตัวโดยการตัดแปลงจากทฤษฎีการวัดประสิทธิภาพของกระบวนการทางสถิติ [8] ดังสมการที่ (3)

$$Feature_{cap} = Cpk_{Genuine} - Cpk_{Impost} \quad (3)$$

CpkGenuine : คือค่าความสามารถเฉลี่ยของ Feature แต่ละตัวของเจ้าของ Username ที่แท้จริง โดยใช้ Username 30 ครั้งของเจ้าของเปรียบเทียบกับค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของ Username 10 ครั้งแรกที่จะนำมาเป็นต้นแบบ CpkImpost: คือค่าความสามารถเฉลี่ยของ Feature แต่ละตัวของผู้โจมตี

ทั้ง 3 โดยใช้ Username 30 ครั้งจากผู้โจมตีเปรียบเทียบกับค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของ Username 10 ครั้งแรกของเจ้าของ Username ที่จะนำมาเป็นต้นแบบ สมการวัดความสามารถข้างต้นได้ประยุกต์มาจากสมการมาตรฐานทางสถิติ [8] ดังสมการที่ 4

$$Cpk = \min(Cpu, Cpl) , Cpu = \frac{USL - \bar{X}_A}{3\sigma_A} , Cpl = \frac{\bar{X}_A - LSL}{3\sigma_A}$$

$$USL = \bar{X}_B + 3\sigma_B , LSL = \bar{X}_B - 3\sigma_B \quad (4)$$

Cpk : ค่าความสามารถของกระบวนการที่แสดงถึงความใกล้เคียงกับเป้าหมายและการควบคุมความแปรปรวนของกระบวนการ Cpk ที่มีค่าสูงแสดงถึงความสามารถในการควบคุมกระบวนการที่ดี Cpu: ค่าความสามารถของกระบวนการทางด้านขีดจำกัดบนของค่าเป้าหมาย โดยบ่งบอกถึงประสิทธิภาพในการควบคุมความแปรปรวนและการเข้าใกล้ค่าเป้าหมายของกระบวนการ Cpl: ค่าความสามารถของกระบวนการทางด้านขีดจำกัดล่างของค่าเป้าหมาย โดยบ่งบอกถึงประสิทธิภาพในการควบคุมความแปรปรวนและการเข้าใกล้ค่าเป้าหมายของกระบวนการ USL : คือค่าขีดจำกัดบนของค่าเป้าหมาย

หมายถึงคำนวณจากค่าเฉลี่ยของเป้าหมายบวกด้วย 3 เท่าของค่าเบี่ยงเบนมาตรฐานของชุดข้อมูลที่เป็นต้นแบบ LSL : ค่าขีดจำกัดล่างของค่าเป้าหมายซึ่งคำนวณจากค่าเฉลี่ยของเป้าหมายลบด้วย 3 เท่าของค่าเบี่ยงเบนมาตรฐานของชุดข้อมูลที่เป็นต้นแบบ  $\bar{X}_A, \sigma_A$  ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของข้อมูลที่ต้องการประเมินความสามารถของกระบวนการ  $\bar{X}_B, \sigma_B$ : ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของข้อมูลที่ใช้อ้างอิงและเป็นเป้าหมายในการประเมินความสามารถของกระบวนการ ดังนั้น Feature ที่ถูกเลือกจะต้องมีค่า FeatureCap สูงที่สุดสองอันดับแรก และนำมาใช้สร้างเส้นโคจร เนื่องจากแสดงให้เห็นว่ามีค่าความสามารถของเจ้าของดีกว่าผู้โจมตีมากที่สุดซึ่งหมายถึงการคัดแยกระหว่างเจ้าของและผู้โจมตีที่มีความชัดเจน ซึ่งส่งผลให้การพิสูจน์ตัวตนมีประสิทธิภาพสูงที่สุด ผู้วิจัยได้ทดลองทฤษฎีดังกล่าวกับข้อมูลของอาสาสมัคร 3 คน จากผลการทดลองทำให้ Feature “I/1000” และ “L/1000” ถูกเลือก เนื่องจากให้ค่า FeatureCap สูงเป็นสองอันดับแรกของอาสาสมัคร 2 ใน 3 คนให้ผลลัพธ์ดังตารางที่ 1

ตารางที่ 1 ผลลัพธ์จากการวัดความสามารถ Feature

|      | H/1000                             | I/1000                             | L/1000                             | H/Total                            | I/Total                            | L/Total                            | H/Sum H                            | I/Sum I                            | L/Sum L                            |
|------|------------------------------------|------------------------------------|------------------------------------|------------------------------------|------------------------------------|------------------------------------|------------------------------------|------------------------------------|------------------------------------|
| Key  | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> |
| m    | -0.36058                           | -0.304214                          | 1.109704                           | 0.979213                           | 0.095894                           | -0.06855                           | -0.13229                           | 0.242791                           | -0.1644468                         |
| a    | 1.560046                           | 0.490939                           | 1.369627                           | 0.85021                            | -0.7401                            | -0.2841                            | 1.277662                           | 0.147029                           | -0.1249769                         |
| y    | -0.02907                           | 0.097267                           | 0.347532                           | 0.901099                           | 1.738216                           | 2.205524                           | -0.08004                           | 2.135042                           | 2.3821954                          |
| t    | 0.02545                            | 6.922116                           | 6.631409                           | 1.383942                           | 3.737411                           | 2.290478                           | 0.953804                           | 2.224876                           | 2.0955769                          |
| i    | 0.36153                            | 1.7857                             | 1.439236                           | 1.383942                           | 0.719368                           | 1.279254                           | 1.349523                           | 1.129244                           | 1.3837314                          |
| n    | 0.083146                           | 2.054448                           | 1.808456                           | 1.707304                           | 0.742636                           | 0.165086                           | 0.681772                           | -0.00154                           | 0.0728593                          |
| e    | 0.278113                           | 0.98673                            | 1.086271                           | 1.299673                           | 1.224506                           | 1.150162                           | 0.109386                           | 1.230092                           | 1.1701512                          |
| e    | 0.501015                           | 1.862484                           | 2.018295                           | 0.955634                           | 2.072566                           | 1.552667                           | 0.06433                            | 1.276203                           | 1.4368463                          |
| a    | 0.815925                           |                                    |                                    | 1.33995                            |                                    |                                    | 0.454446                           |                                    |                                    |
| Mean | 0.359505                           | 1.736934                           | 1.976316                           | 1.200108                           | 1.198812                           | 1.036315                           | 0.519844                           | 1.047967                           | 1.0314921                          |
| Key  | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> |
| k    | 1.184261                           | 1.226967                           | 1.927648                           | 1.426691                           | 0.946234                           | 1.114615                           | 0.123126                           | -0.47602                           | 1.3175875                          |
| a    | 0.582069                           | 1.544231                           | 1.562174                           | 1.517218                           | 1.223006                           | 0.823206                           | 0.316769                           | 0.370572                           | 0.8208335                          |
| s    | 0.665347                           | 1.490308                           | 1.440941                           | 1.11209                            | 1.355439                           | 0.550162                           | 0.439122                           | -2.33986                           | 0.4903295                          |
| e    | 0.671353                           | 1.071235                           | 1.293856                           | 0.49748                            | 0.568472                           | 0.662531                           | -0.16437                           | 3.887512                           | 0.7462871                          |
| m    | 0.276431                           | 1.21036                            | 1.659883                           | 0.915424                           | 0.945425                           | 0.364468                           | -0.01915                           | -0.29485                           | 0.2547701                          |
| w    | 0.963228                           |                                    |                                    | 1.197444                           |                                    |                                    | 0.52561                            |                                    |                                    |
| Mean | 0.723782                           | 1.30862                            | 1.5769                             | 1.111058                           | 1.007715                           | 0.702997                           | 0.203518                           | 0.229469                           | 0.7259615                          |
| Key  | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> | Feature <sub>C<sub>key</sub></sub> |
| k    | 1.535257                           | 2.182462                           | 1.083272                           | 4.377939                           | 1.871519                           | -0.06032                           | 0.027115                           | -1.38271                           | 0.1768394                          |
| a    | 0.465614                           | 1.238641                           | 1.581689                           | 2.651893                           | 1.076155                           | 0.583617                           | -0.18258                           | 0.073545                           | 0.5621543                          |
| m    | 0.842666                           | 2.88113                            | 1.510472                           | 3.899972                           | 0.5431                             | -0.05117                           | 0.181099                           | -0.81203                           | 0.3591644                          |
| o    | -0.43944                           | 1.372741                           | 1.524724                           | 2.358768                           | -1.50583                           | 2.020001                           | 0.512915                           | 0.013997                           | 2.3763859                          |
| l    | 1.213222                           | 2.546579                           | 2.112816                           | 5.457015                           | 3.170764                           | 1.987929                           | -0.34219                           | -0.11399                           | 1.9287246                          |
| r    | 0.716238                           | 1.370327                           | 1.001104                           | 3.862401                           | 1.413568                           | 0.408758                           | -0.12738                           | 0.232467                           | 0.3480523                          |
| a    | 0.507047                           | 2.090275                           | 1.700646                           | 3.598043                           | 2.371989                           | 0.282159                           | -0.19565                           | -0.08177                           | 0.0922799                          |
| t    | 2.760893                           | 1.985776                           | 1.250703                           | 10.08852                           | 2.597761                           | 0.609065                           | 1.572571                           | 0.201336                           | 0.9566947                          |
| s    | -1.26444                           |                                    |                                    | 0.366567                           |                                    |                                    | 0.000686                           |                                    |                                    |
| Mean | 0.705638                           | 1.958492                           | 1.470678                           | 4.073458                           | 1.442378                           | 0.722505                           | 0.160732                           | -0.23364                           | 0.8050369                          |

## 7. การทดสอบผลการพิสูจน์ตัวตน

จากการคัดเลือก Feature เพื่อนำมาประกอบเป็นเส้นโครงที่คาดว่าจะให้ผลการพิสูจน์ตัวตนที่ดีที่สุดจาก Feature ที่มีอยู่ทั้งหมด ผู้วิจัยได้สร้างโปรแกรมประยุกต์ด้วยภาษา C# ดังภาพที่ 6 เพื่อประมวลผลข้อมูลจากอาสาสมัคร 20 คน และผู้โจมตี 3 คน โดยผู้วิจัยกำหนดให้โปรแกรมทำการจัด Feature สร้างเส้นโครง และระบุตัวตนโดยปรับค่า Allowance Factor จนได้ค่า EER (Equal Error Rate) ซึ่งคือ FRR (False Rejection Rate) และ FAR (False Acceptance Rate)[1] [17] ให้มีค่าเท่ากันหรือใกล้เคียงกันมากที่สุด โดยจะสร้างเส้นโครงจากทุก Feature โดยการจับคู่ที่เป็นไปได้ทุกคู่ จากนั้นจึงดำเนินการพิสูจน์ตัวตน ซึ่งผลลัพธ์จากวิธีการดังกล่าวพบว่าการเลือก Feature “I/1000” และ “L/1000” มาจัดเป็นโครงสร้างเส้นโครง และพิสูจน์ตัวตนด้วยวิธีการวัดความแตกต่างของเส้นโครงให้ผลลัพธ์ที่ดีที่สุดจาก Feature ทั้งหมด และตรงตามที่ผู้วิจัยได้คัดเลือกโดยให้ค่าผลการทดลองที่  $ERR = 4\%$  ( $FAR=4\%$ ,  $FRR=4\%$ ) ที่ Allowance Factor = 2.76 หมายความว่าระบบพิสูจน์ตัวตนมีความแม่นยำถึง 96%



ภาพที่ 6 โปรแกรมประยุกต์ทดสอบการพิสูจน์ตัวตน

## 8. เปรียบเทียบผลการทดลอง

จากงานวิจัยที่เกี่ยวข้องพบว่าผลการทดลองของงานวิจัยนี้ให้ผลลัพธ์ที่ดีกว่างานวิจัยหลายงาน ซึ่งงานวิจัยที่นำมาเปรียบเทียบใช้วิธีการวัดประสิทธิภาพด้วย Equal Error Rate (ERR) เช่นเดียวกับงานวิจัยชิ้นนี้ และได้แสดงผลการเปรียบเทียบดังตารางที่ 2 อย่างไรก็ตามพบว่ายังมีงานวิจัยอื่นๆ อีก ที่ให้ผลการพิสูจน์ตัวตนที่ดีกว่าเช่น Kang, Hwang, Cho [5], Hwang, Lee, Cho [18] และ Jiang, Shieh, Liu [19] โดยใช้เทคนิคขั้นสูงในการประมวลผล และใช้จำนวนข้อมูลที่ค่อนข้างมากเช่น Jiang, Shieh และ Liu [19] ใช้เทคนิค Hidden Markov Models และใช้จำนวนข้อมูลของอาสาสมัคร 58 คน และใช้จำนวนตัวอย่างข้อมูลในการทำต้นแบบ 20 ตัวอย่างต่ออาสาสมัคร 1 คน โดยให้ผล Error Rate ที่ 2.54% ซึ่งถ้าเทียบกับงานวิจัยชิ้นนี้ใช้จำนวนอาสาสมัคร 20 คนและต้องการข้อมูลการทำต้นแบบเพียง 10 ตัวอย่าง อีกทั้งยังใช้หลักการไม่ซับซ้อนซึ่งทำให้เข้าใจและเห็นภาพได้ง่าย รวมทั้งยังให้ผลลัพธ์ Error Rate 4% ซึ่งต่างจากงานวิจัยที่กล่าวถึงเพียง 1.46% อย่างไรก็ตามงานวิจัยนี้มีจุดอ่อนในด้านที่ไม่มีการเรียนรู้และปรับเส้นโครงต้นแบบอย่างต่อเนื่องเมื่อเวลาผ่านไป ดังนั้นหากผู้ใช้งานมีพฤติกรรมการพิมพ์ที่เปลี่ยนไปจากเดิมอาจส่งผลให้ระบบการพิสูจน์ตัวตนมีประสิทธิภาพลดลง แต่งานวิจัยนี้มีความน่าสนใจตรงที่มีความเรียบง่ายไม่ซับซ้อนจนเกินไปซึ่งเหมาะสำหรับการนำไปประยุกต์ใช้งานในระบบจริง

ตารางที่ 2 เปรียบเทียบประสิทธิภาพกับ  
งานวิจัยที่เกี่ยวข้อง

| Author                                             | Ref Paper | Technique                | ERR(%) |
|----------------------------------------------------|-----------|--------------------------|--------|
| Proposed Technique                                 | N/A       | Trajectory Dissimilarity | 4%     |
| M. Brown, S.J. Rogers                              | [10]      | Kohonen and MLP          | 4.2    |
| L.Taweetham                                        | [1]       | Advance Stat.            | 5.24   |
| Steven M.Walker                                    | [9]       | N/A                      | 5.4    |
| R. Giot, M. El-Abed,<br>and C. Rosenberger         | [15]      | SVM                      | 6.96   |
| D. Tran, W. Ma, G. Chetty,<br>and D. Sharma        | [13]      | Markov and Fuzzy         | 8.6    |
| J.R. Montalv ao Filho, E.O. Freire                 | [12]      | Hidden Markov Models     | 12.7   |
| E. Maiorana, P. Campisi,<br>N. Gonz 'alez-Carbalo, | [16]      | KNN                      | 14     |
| F. Monrosec, A. Rubin                              | [11]      | KNN                      | 15.4   |
| M. Rybnik, M. Tabezki,<br>and K. Saeed             | [14]      | Vote                     | 24.22  |

## 9. สรุปผลการทดลอง

จากผลการทดลองพบว่าทฤษฎีการคัดเลือก Feature ของผู้วิจัยและระบบการพิสูจน์ตัวตนที่ผู้วิจัย ได้คิดค้นด้วยวิธีการวัดความต่างของเส้นโคจร โดยนำ ข้อมูล Keystroke Dynamics มาจัดรูปเป็นเส้นโคจร จากนั้นวัดความแตกต่างจากเส้นโคจรต้นแบบของ เจ้าของที่แท้จริง วิธีการดังกล่าวถือว่าให้ผลความ แม่นยำสูง โดยให้ค่าความผิดพลาด EER ที่ 4% หรือ แม่นยำถึง 96% ซึ่งงานวิจัยนี้ได้แสดงให้เห็นถึง แนวทางและประโยชน์ของการนำพฤติกรรมของ มนุษย์มาประยุกต์ใช้ในศาสตร์ทางด้านความมั่นคงบน ระบบคอมพิวเตอร์ซึ่งสามารถลดจุดอ่อน และเพิ่ม

ความแข็งแกร่งให้กับการพิสูจน์ตัวตนบนระบบ คอมพิวเตอร์ได้อย่างมีประสิทธิภาพ

## 10. งานวิจัยในอนาคต

จากจุดอ่อนของงานวิจัยนี้ที่ได้กล่าวข้างต้นทำให้ ผู้วิจัยมีความสนใจที่จะวิจัยถึงการรักษาประสิทธิภาพ ของระบบเมื่อเวลาผ่านไป โดยการเพิ่มระบบการเรียนรู้ และปรับปรุงเส้นโคจรต้นแบบ หากผู้ใช้มีพฤติกรรม การพิมพ์ที่เปลี่ยนไป ซึ่งทำให้มีความน่าสนใจและเป็น ไปได้ที่จะสามารถนำการพิสูจน์ตัวตนด้วย Keystroke Dynamics ไปใช้งานได้ในระบบจริง ถึงแม้ว่ายังมีค่า ความผิดพลาดอยู่บ้าง แต่ถือว่าน้อยมาก เช่นการนำไป ใช้บนโทรศัพท์มือถือหรือคอมพิวเตอร์แบบพกพา ซึ่งเป็นที่นิยมในปัจจุบัน เพราะจะนำไปช่วยเสริม ระบบความปลอดภัยบนอุปกรณ์พกพาเหล่านั้น

## 11. กิตติกรรมประกาศ

ขอขอบคุณ อาสาสมัครจำนวน 23 ท่านที่สละ เวลาให้ความช่วยเหลือในการเก็บข้อมูล ขอขอบคุณ นักวิจัย Mr.Romain Giot และ Mr.Daniele Gunetti ซึ่งเชี่ยวชาญทางด้านนี้ได้เสียสละเวลาให้คำแนะนำ รวมถึงมอบตัวอย่างข้อมูลให้ผู้วิจัยได้ทำการศึกษาซึ่งเป็นประโยชน์อย่างยิ่ง

## เอกสารอ้างอิง

- [1] Taweetham Limpanuparb "The Enhancement of Password Security System Using Key Stroke Verification" Congress on Science and Technology of Thailand ,2004
- [2] S. Haider, A. Abbas, and A. K. Zaidi. "A multi-technique approach for user identification through keystroke dynamics." IEEE International Conference on Systems, Man and Cybernetics, pp.1336-1341, 2000.
- [3] K.Senathipathi, K.Batri "Keystroke Dynamics Based Human Authentication System using Genetic Algorithm" European Journal of Scientific Research ,Vol.82, pp.446-459, 2012
- [4] Y.Kaneko, Y.Kinpara, Y.Shinomi "A Hamming Distance-like In Keystroke Dynamics" Ninth Annual International Conference on Privacy, Security and Trust, 2011

- [5] P.Kang, S.Hwang, S.Cho “Continual Retrain of Keystroke Dynamics Based Authenticator” Springer-Verlag Berlin Heidelberg, pp.1203-1211, 2007
- [6] P.Laurinen, P. Siirtola, and J.Roning ”Efficient Algorithm for Calculating Similarity Between Trajectories Containing an Increasing Dimension” International Conference of Artificial Intelligence and Application, P.392-399, 2006
- [7] สมจิตร วัฒนายากุล ”สถิติพื้นฐานสำหรับนักวิทยาศาสตร์” สำนักพิมพ์ประกายพริ้ง, 2003
- [8] Pande, P. N. “The six sigma: how GE, Motorola and other top companies are honing their performance.” Mc. Graw-Hill. USA: 2000
- [9] Steven M. Walker “Biometric Selection: Body Parts Online” SANS Institute Reading Room, 2002
- [10] M. Brown and S.J. Rogers.”User identification via keystroke characteristics of typed names using neural networks” International Journal of ManMachineStudies,39(6), pp.999–1014, 1993.
- [11] F. Monroe and A. Rubin. “Authentication via keystroke dynamics.” In The 4th ACM conference on Computer and communications security, CCS 1997, pages 48– 56, New York, NY, USA, 1997. ACM.
- [12] R. Montalv ao Filho and E.O. Freire. On the “Equalization of keystroke timing histograms.” Pattern Recognition Letters, 27(13), pp.1440–1446, 2006.
- [13] D. Tran, W. Ma, G. Chetty, and D. Sharma. “Fuzzy and markov models for keystroke biometrics authentication”. In The 7th WSEAS International Conference on Simulation, Modeling and Optimization, SMO 2007, pp.89–94, Stevens Point, Wisconsin, USA, 2007. World Scientific and Engineering Academy and Society (WSEAS).
- [14] M. Rybnik, M. Tabedzki, and K. Saeed. “A keystroke dynamics based system for user identification.” In The7th Computer Information Systems and Industrial Management Applications, CISIM 2008, pp.225–230, June 2008.
- [15] R. Giot, M. El-Abed, and C. Rosenberger. “Keystroke Dynamics with low constraints svm based passphrase enrollment.” In The 3rd IEEE international conference on Bio-metrics : Theory, applications and systems, BTAS 2009, pp.425–430, Piscataway, NJ, USA, 2009. IEEE Press.
- [16] E. Maiorana, P. Campisi, N. Gonz´alez-Carballo, and A. Neri. “Keystroke dynamics authentication for mobile phones.” In The 2011 ACM Symposium on Applied Computing, SAC 2011, pp.21–26, New York, NY, USA,2011. ACM.
- [17] R.Gio, M.El-Abed and C.Rosenberger “Web-Based Benchmark for Keystroke Dynamics Biometric Systems: A Statistical Analysis” IEEE Conference Publication, pp.11-15,2012
- [18] S.-s. Hwang, H.-j. Lee, and S. Cho. “Improving authentication accuracy using artificial rhythms and cues for keystroke dynamics-based authentication.” Expert Systems with Applications: An International Journal, 36(7), pp.10649–10656, 2009.
- [19] C.-H. Jiang, S. Shieh, and J.-C. Liu. Keystroke Statistical learning model for web authentication. In The 2nd ACM symposium on Information, computer and communications security, ASIACCS 2007, pp.359–361, New York, NY, USA, 2007. ACM.